PATENT COOPERATION TREA Y

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/JP2005/002514	10.02.2005	10.02.2004

International Patent Classification (IPC) or both national classification and IPC
H04L9/08

Applicant
NTT COMMUNICATIONS CORPORATION

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☒ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA"). However, this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of three months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA:

European Patent Office - P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk - Pays Bas
Tel. +31 70 340 - 2040 Tx: 31 651 epo nl
Fax: +31 70 340 - 3016

Authorized Officer

Dujardin, C

Telephone No. +31 70 340-2840

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/JP2005/002514

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

   ☐ This opinion has been established on the basis of a translation from the original language into the following language , which is the language of a translation furnished for the purposes of international search (under Rules 12.3 and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

   a. type of material:

   ☐ a sequence listing

   ☐ table(s) related to the sequence listing

   b. format of material:

   ☐ in written format

   ☐ in computer readable form

   c. time of filing/furnishing:

   ☐ contained in the international application as filed.

   ☐ filed together with the international application in computer readable form.

   ☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non obvious), or to be industrially applicable have not been examined in respect of:

☐ the entire international application,

☒ claims Nos. 7-14

because:

☐ the said international application, or the said claims Nos. relate to the following subject matter which does not require an international preliminary examination *(specify)*:

☒ the description, claims or drawings *(indicate particular elements below)* or said claims Nos. 7-14 are so unclear that no meaningful opinion could be formed *(specify)*:

see separate sheet

☒ the claims, or said claims Nos. 7-14 are so inadequately supported by the description that no meaningful opinion could be formed.

☐ no international search report has been established for the whole application or for said claims Nos.

☐ the nucleotide and/or amino acid sequence listing does not comply with the standard provided for in Annex C of the Administrative Instructions in that:

the written form	☐	has not been furnished
	☐	does not comply with the standard
the computer readable form	☐	has not been furnished
	☐	does not comply with the standard

☐ the tables related to the nucleotide and/or amino acid sequence listing, if in computer readable form only, do not comply with the technical requirements provided for in Annex C-*bis* of the Administrative Instructions.

☐ See separate sheet for further details

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-6,15,16
	No:	Claims	
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-6,15,16
Industrial applicability (IA)	Yes:	Claims	1-6,15,16
	No:	Claims	

2. Citations and explanations

see separate sheet

Re Item III

Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

1. Claim 7, as well as claims 8-10, is unclear and unsupported by the description (Article 6 PCT) for the reasons exposed in the paragraphs 1.1. to 1.3. below. Claims 8-14, which are dependent on claim 7, contain all features of claim 7 and are therefore also unclear and unsupported by the description. Hence, it has not been possible to examine claims 7-14.

1.1. The expression "secret sharing scheme which is" used in claim 7 appears to introduce a definition of "secret sharing scheme" which is not the definition generally accepted. In particular, the passage "according to a desired processing unit bit length" is unclear and does not correspond to the usual definition of secret sharing scheme.

1.2. In the wording of claim 7, there seem to be some confusion between the division into divided data using the secret sharing scheme and the division into partial data according to a desired processing unit length, for example in the following passages: " dividing the secret information into the divided data in a desired number of division according to a desired processing unit bit length" and "generating each divided partial data [...] by calculating exclusive OR of the original partial data and the random number partial data".

In this respect, the latter expression seems to suggest that each divided partial data is calculated by the following formula (using the same notations as in the present application): $D(i,j)=S(j) * R(j)$ for any i, which would mean that all divided partial data are identically calculated. This is however inconsistent with the embodiments of the description (see e.g. figure 7). Claim 7 is therefore unclear (Article 6 PCT) and lacks support from the description (Article 6 PCT).
It is to be noted that a similar objection can be raised, mutatis mutandis, against claims 8-10, which also contain expressions that render the operands of the exclusive OR operation unclear.

1.3. Moreover there appears to be a missing passage in claim 8, since the expression "exclusive OR of" is only followed by a single operand whereas an exclusive OR operation normally operates on two operands. Claim 8 is therefore unclear (Article 6 PCT).

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

2. Reference is made to the following document:
D1: US-A-5 675 649 (BRENNAN ET AL) 7 October 1997 (1997-10-07)

3. The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of independent claims 1, 15 and 16 does not involve an inventive step in the sense of Article 33(3) PCT.

3.1. The document D1 (the references in parentheses applying to this document) is regarded as being the closest prior art to the subject-matter of claim 15, and discloses (column 3, line 28 - column 6, line 10, figures 2-3) a secret information management method for managing a secret information (master key) of a user, comprising the steps of:

- dividing the secret information into a plurality of divided data (master key shares) by using a secret sharing scheme, such that the secret information can be recovered from a prescribed number of the divided data (column 5, lines 28-35; figure 2, step 44);
- storing the plurality of divided data into a plurality of deposit agent disks (column 4, lines 47-46; column 5, lines 36-37; figure 2, step 48);
- generating a plurality of re-divided data different from the plurality of divided data obtained by the dividing step, from a combination of the prescribed number of the divided data among the divided data stored in the deposit servers by using the secret sharing scheme (column 5, lines 58-61; column 6, lines 1-4; figure 3, steps 60 and 70); and
- storing the plurality of re-divided data into the deposit agent disks as newly generated divided data (column 4, line 61 - column 5, line 3; column 6, lines 4-

10; figure 3, step 74).

The subject-matter of claim 15 therefore differs from this known method in that

A) the user (i.e. the owner of the secret information) is one of the deposit agents and, as such, receives a part of the plurality of divided data.

B) each deposit agent (including the user) stores his part of the divided data into a corresponding server (or terminal), instead of storing it on a portable disk.

The problem to be solved by A) may be regarded as increasing the trust of the owner of the secret information in the deposit agents.

The solution proposed in claim 15 of the present application cannot be considered as involving an inventive step for the following reasons:

- Although feature A) is not explicitly mentioned in D1, nothing in the teaching of D1 allows to exclude the possibility of having feature A) included in the method of D1.
- It is clearly mentioned in D1 (column 3, lines 40-48; column 14, lines 1-8) that the security of the secret information depends on the reliability of the deposit agents and, since the selection of the deposit agents and the assessment of their reliability is achieved by the owner of the secret information, relies on the trust placed by the owner of the secret information in the deposit agents.
- It is generally assumed that the user considers himself as being above suspicion and is the person who has the least interest in intentionally compromising his part of the divided data or in neglecting securing it. And therefore it would be obvious for the skilled person to increase the trust of the owner of the secret information in one deposit agent, and therefore in the set of deposit agents as a whole, by having the owner select himself as one of the deposit agents.

As far as feature B) is concerned, it is generally known to the person skilled in the art that the feature of storing data in the memory of a server or terminal is an obvious alternative to the feature of storing data on a portable disk, and can be interchanged with that feature where circumstances make it desirable.

There is no interaction between features A) and B) and their contributions to the prior art, when considered individually, are regarded (see reasoning above) as being obvious to a person skilled in the art. Therefore, the subject-matter of claim 15 does not involve an inventive step (Article 33(3) PCT).

3.2. The same reasoning applies, mutatis mutandis, to the subject-matter of the corresponding independent claims 1 and 16, which therefore are also considered not inventive.

4. Dependent claims 2-6 do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of inventive step, see documents and passages cited in the search report.